ASSEMBLY BILL No. 670

Introduced by Assembly Member Irwin

February 25, 2015

An act to amend Section 11549.3 of the Government Code, relating to technology.

LEGISLATIVE COUNSEL'S DIGEST

AB 670, as introduced, Irwin. Security assessments.

Existing law establishes the Department of Technology within the Government Operations Agency, headed by the Director of Technology who is also known as the State Chief Information Officer. The department is responsible for the approval and oversight of information technology projects by, among other things, consulting with agencies during initial project planning to ensure that project proposals are based on well-defined programmatic needs.

Existing law establishes the Office of Technology Services within the department, under the supervision of the Chief of the Office of Technology Services, and sets forth its duties, including, but not limited to, the authority to conduct or require a security assessments of any state agency, as prescribed.

This bill would, instead, require the office to conduct, or require, an assessment of every state agency at least once every 2 years and would require the state agency being audited to pay the costs of the security assessment. The bill would authorize the department to require agencies that are not in compliance to redirect available funding to pay the costs of the assessments. The bill would require the department to adopt standards, to be included within the State Administrative Manual, setting

forth the manner for the assessed agency to communicate the assessment results to the department.

This bill would authorize the department and the Governor's Office of Emergency Services to jointly conduct the strategic direction of risk assessments performed by the Military Department's Computer Network Defense Team.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 11549.3 of the Government Code is amended to read:

11549.3. (a) The director shall establish an information security program. The program responsibilities include, but are not limited to, all of the following:

(1) The creation, updating, and publishing of information security and privacy policies, standards, and procedures for state agencies in the State Administrative Manual.

(2) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies to effectively manage security and risk for both of the following:

(A) Information technology, which includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, and all related interactions between people and machines.

(B) Information that is identified as mission critical, confidential, sensitive, or personal, as defined and published by the Office of Information Security.

(3) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies for the collection, tracking, and reporting of information regarding security and privacy incidents.

(4) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies in the development, maintenance, testing, and filing of each agency's disaster recovery plan.

(5) Coordination of the activities of agency information security officers, for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards.

(6) Promotion and enhancement of the state agencies' risk management and privacy programs through education, awareness, collaboration, and consultation.

(7) Representing the state before the federal government, other state agencies, local government entities, and private industry on issues that have statewide impact on information security and privacy.

(b) An information security officer appointed pursuant to Section 11546.1 shall implement the policies and procedures issued by the Office of Information Security, including, but not limited to, performing both of the following duties:

(1) Comply with the information security and privacy policies, standards, and procedures issued pursuant to this chapter by the Office of Information Security.

(2) Comply with filing requirements and incident notification by providing timely information and reports as required by policy or directives of the office.

(c) ~~(1) Except as provided in paragraph (2), the office may~~ *The office shall* conduct, or require to be conducted, *an* independent security ~~assessments~~ *assessment* of ~~any~~ *every* state agency, department, or ~~office, the~~ *office at least once every two years. The* cost of ~~which~~ *the security assessment* shall be funded by the state agency, department, or office being assessed. *The assessment shall include, at a minimum, all of the following components, which shall be conducted in compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Controls:*

(1) A legal, policy, standards, and procedure compliance review.

(2) Vulnerability scanning.

(3) Penetration testing.

~~(2) The office shall not conduct, or require to be conducted, independent security assessments of the Department of Forestry and Fire Prevention.~~

~~(d) The office may require an audit of information security to ensure program compliance, the cost of which shall be funded by the state agency, department, or office being audited.~~

~~(e)~~

(d) The office shall report to the Department of Technology any state agency found to be noncompliant with information security program requirements.

(e) The Department of Technology may require that any agency in noncompliance with subdivision (c) redirect any funds within the agency's budget, that may be legally expended for these purposes, for the purposes of paying the costs of compliance with subdivision (c).

(f) The Department of Technology and the Governor's Office of Emergency Services may jointly conduct the strategic direction of risk assessments performed by the Military Department's Computer Network Defense Team, as budgeted in Item 8940-001-0001 of the Budget Act of 2014.

(g) The Department of Technology shall adopt standards, to be included within the State Administrative Manual, setting forth the manner for the assessed agency to communicate the assessment results to the department, including, but not limited to, all of the following:

(1) Identification of vulnerabilities.

(2) Prioritization of vulnerabilities.

(3) Identification of relevant internal resources.

(4) Strategy for addressing and mitigating those vulnerabilities.

O